CHAPTER 6 Security Organization

Information security is no longer simply about patch management and firewalls. It requires a holistic risk management approach. As organizations increasingly rely on global networks for supply chain and communications, and amass distributed data in terabyte amounts, it has become apparent that the old models for computer security are no longer effective. The exploitation points have correspondingly increased exponentially. The old model of hiring a couple of security analysts or engineers and throwing them into the Information Technology department is no longer sufficient to address the growing needs of data and communications protection. Security can no longer be left in the hands of the technologists. It must be acknowledged, considered, embraced, and championed at the highest levels of the organization. In other words, it must be aligned to the business objectives of the organization to maintain or improve its value.

What is now required is a risk management approach to security that addresses the organization as a whole. Risk management cannot be conducted in a silo. It requires a coordinated and collaborative approach throughout the organization and must be lifecycle oriented. It is not enough to form a "security department" by putting somebody in charge, hiring a few security technologists, and calling it a day. Security risk management must now evolve into a highly defined, quantifiable, justifiable approach to securing the organization's assets and reputation against loss. That "ultimate responsibility" lands on the shoulders of top executives.

So why the change? Now that the Information Age has permeated all aspects of the business world, the business environment and the information that drives it have become increasingly dynamic. The information landscape changes daily, and organizations need to adapt to that change to protect their assets—in other words, manage their risk.

Roles and Responsibilities

At the executive level, there must be overall and/or ultimate responsibility (or accountability, if you prefer) for risk management. The size of the risk management organization headed by that executive will vary based on the size of the business. Large organizations may have all the roles that are defined in this chapter, whereas smaller organizations may employ a security organization that consists of a few individuals (who may also share other responsibilities, as long as those responsibilities don't conflict with their security roles). Midsize organizations need several security positions ranging from the technical security administrators who configure firewalls, routers, antivirus software, and the like, to security engineers who design security controls, managed by a security manager, director, or senior executive. Large organizations need a complete security organization. All organizations, large or small, need an executive decision maker who has been designated as being responsible for security risk.

In addition, the distinctions between large and small organizations and what security positions they require vary according to what the organization does. Financial companies typically require a larger and more robust security organization due to the capital financial risk involved in an event or incident that negatively impacts their integrity, confidentiality, and availability. Healthcare organizations, along with businesses in other highly regulated sectors such as publicly traded companies that must comply with Sarbanes-Oxley rules, and financial companies that are regulated by the Gramm-Leach-Bliley Act, also require a substantial security organization. Technology companies may require a midsize or smaller security organization, depending on how exposed they are to threats, vulnerabilities, and risks from an attack and how much their security posture is improved by aligning security to business objectives. Every organization is different.

Oracle's Chief Security Officer: A Case Study

As Oracle's Chief Security Officer (CSO), Mary Ann Davidson has responsibility for product security as well as security policies, the security of infrastructure, security evaluations and assessments, and incident handling. Oracle was one of the first companies to establish a CSO position, along with a Chief Privacy Officer (CPO). While their offices operate independently, these senior executives coordinate their efforts on security and privacy issues.

Davidson maintains that software manufacturers should design and build their applications securely. To do this, she proposes the following:

- Develop a core group of security experts to inject security into application design
- Centralize common security functions to work together
- Develop secure coding practices to avoid common vulnerabilities
- Conduct regression testing to ensure that new versions of software don't invalidate previous security controls
- Submit to independent product assessments and security evaluations such as the Common Criteria testing program sponsored by the National Institute of Standards (NIST) and the National Security Agency (NSA)

The ability to influence corporate culture at this level demonstrates the effectiveness and value of an officer-level security position.

Security Positions

The following positions are recommended for security organizations. Other positions also exist outside the formal security organization, because everyone in the business has some level of responsibility for security. For example, every employee is responsible for protecting their passwords, their login sessions, and any confidential information they handle. General managers, department heads, and operational leads are responsible for being familiar with security policy and keeping an eye on the security practices of their subordinates. They are responsible for ensuring that violations are reported, and may carry out enforcement policies.

Figure 6-1 shows an example security responsibility hierarchy, with some descriptions of responsibilities that might pertain to each position.

Chief Security Risk Officer (CSRO) or Chief Information Security Officer (CISO)

This position is an executive staff member, with ultimate accountability for all security efforts for the business. The CSRO oversees all aspects of risk management across the enterprise, or in organizations without a formal risk management department, the CISO oversees the information security function and incorporates risk management into that function. In organizations where the CSRO is responsible for all types of risks across the business (including financial risks, business risks, and other non-IT risks), the person in that role will generally establish an IT risk function to oversee IT-related risks in particular, since the management of IT risks represents a unique discipline requiring specialized knowledge. Otherwise, the CISO performs that role. The CSRO or CISO should report to the chief executive officer (CEO), chief operating officer (COO), or the Board of Directors. While some organizations may consider it controversial to elevate the position to equal par with chief executives, the criticality of addressing corporate risk and legal compliance justifies the decision. The CSRO or CISO is a champion and defender of security and risk initiatives for the business, bearing overall responsibility for risk assessment and risk management. The CRSO or CISO may hold certifications related to information security, audit, risk management, and disaster recovery.

In collaboration with the executive staff, the CSRO or CISO should:

- Ensure the business has risk management skills in its human capital
- Establish an organizational structure that supports a risk management strategy
- Implement an integrated risk management framework
- Define the business' risk appetite in terms of loss tolerance
- Ensure the business can absorb the risk in terms of human and financial resources
- Establish risk assessment, management, response, mitigation, and audit procedures
- Influence the business' risk culture and provide organizational learning opportunities

Security Director

The security director works with the executive team to accomplish business goals. This position requires expert communication, negotiation, and leadership skills, as well as technical knowledge of IT and security hardware. While a person who has experience as a

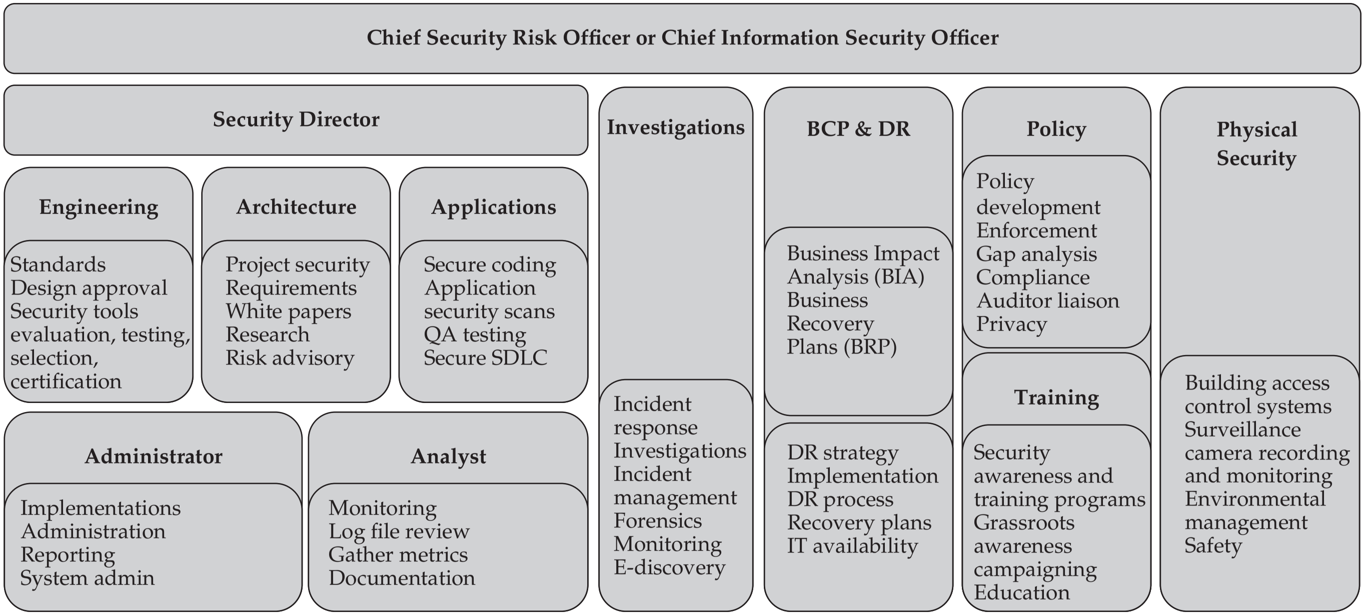

Figure 6-1 Example security organization

vice president may already possess these skills, the focus of the security director should be security-oriented and they should be experienced in information security decision making. The security director has responsibility to oversee and coordinate security efforts across the business, including IT, HR, Communications, Legal, Facilities, and other departments, to identify needed security initiatives and standards.

The security director, among other responsibilities:

- Coordinates the security-related strategic and visionary goals of the business
- Oversees security management and vendors who safeguard the business' assets, intellectual property, and computer systems, as well as the physical safety of employees and visitors
- Identifies protection goals and objectives consistent with corporate strategic plans
- Manages the development and implementation of global security policy (rules), standards (minimum requirements), guidelines (recommendations), and procedures (step-by-step instructions) to ensure ongoing maintenance of security
- Maintains relationships with local, state, and federal law enforcement and other related government agencies
- Oversees the investigation of security breaches and assists with disciplinary and legal matters associated with such breaches as necessary
- Works with outside consultants as appropriate for independent security audits
- Participates in the business' change management process at the organizational and strategic level
- Is fluent with the various aspects of the risk management framework

Security Manager

The security manager has day-to-day responsibility for all security-related activities and incidents. All operational security positions report to this position. The security manager is responsible for management and distribution of the security policy, policy adherence and coordination, and security incident coordination.

The security manager also assigns and determines ownership of data and information systems. In addition, this person also ensures that audits take place to determine compliance with policy. The security manager also makes sure that all levels of management and administrative and technical staff participate during planning, development, and implementation of policies and procedures.

Many of the security manager's functions can be delegated, depending on the staffing requirements and individual skill sets of the security organization. However, the security manager bears accountability for ensuring that these functions take place effectively.

Certifications that a security manager may hold include Information Assurance Manager (IAM) or equivalent and Certified Information Security Manager (CISM) from ISACA.

In addition to other roles, the security manager:

- Develops and maintains a comprehensive security program
- Develops and maintains a business resumption plan for information resources

- Approves access and formally assigns custody of the information resources
- Ensures compliance with security controls
- Plans for contingencies and disaster recovery
- Ensures that adequate technical support is provided to define and select cost-effective security controls

Security Architect

This person has ultimate responsibility for the security architecture, including conducting product testing and keeping track of new bugs and security vulnerabilities as they arise. The security architect produces a detailed security architecture for the network based on identified requirements and uses this architecture specification to drive efforts toward implementation.

In addition to other roles, the security architect:

- Identifies threats and vulnerabilities
- Identifies risks to information resources through risk analysis
- Identifies critical and sensitive information resources
- Works with the data owner to assess and classify information
- Works with technical management to specify cost-effective security controls and convey security control requirements to users and custodians
- Assists the security manager in evaluating the cost-effectiveness of controls

Security Engineer

The primary role of this position is the technical implementation of the architect's designs. The security engineer works directly with the architect on design decisions and with the administrator on device management decisions. Security engineers generally have a degree in engineering or computer science, along with extensive technical training or experience, and they often hold Certified Information Systems Security Professional (CISSP) certification and other technical certifications in their field of expertise.

A security engineer may perform the following duties:

- Installation and configuration of networks and network devices such as web application firewalls, network firewalls, switches, load balancers, and routers
- Security configuration of Unix, Linux, or Windows servers
- Security configuration of applications and databases
- Installation, configuration, and design of security tools, including development and coding
- Security incident investigation, including network packet capture
- Maintenance and monitoring of network and host intrusion detection and prevention technologies

Security Administrator

Every security organization has security administrators, as many as needed to implement security on a day-to-day, operational/tactical basis at the facility. The security administrator executes all actions directed by the security architect, security engineer, security manager, or as required by security policy or incident response procedures. The security administrator is responsible for ensuring all appropriate security requirements are met and maintained on all computers, networks, and network technologies, including patch management and operating system upgrades.

The security administrator is often the first person contacted whenever there is a suspected or known security problem. This person has the operational/tactical responsibility for ensuring that the business, its reputation, and its assets are protected and has the authority to take any and all action necessary to accomplish this goal.

Among other duties, the security administrator:

- Implements the security controls specified by the security architect, security engineer, and security manager
- Implements physical and procedural safeguards for information resources within the facility
- Administers access to the information resources and makes provisions for timely detection, reporting, and analysis of actual and attempted unauthorized access to information resources
- Provides assistance to the individuals responsible for information security
- Assists with acquisition of security hardware/software
- Assists with identification of vulnerabilities and other data gathering activities and log file analysis
- Develops and maintains access control rules
- Maintains user lists, passwords, encryption keys, and other authentication and security-related information and databases
- Develops and follows procedures for reporting on monitored controls

Security Analyst

The primary role of this position is to support the security architect, security engineer, security administrator, and security management in analyzing and producing reports required for the assessment and smooth functioning of security operations. The security analyst may hold vendor-oriented certifications such as those offered by Cisco, Microsoft, Enterasys, Symantec, Oracle, and McAfee.

Among other duties, the security analyst:

- Monitors alerts and reports generated by security systems
- Reviews log files as generated by security devices and servers, making note of anomalies
- Compiles reports as required by management or as specified by security policy
- Maintains security metrics

- Collaborates with security organization team members to assess and analyze security operations and suggests improvement
- Manages quality control and change management initiatives for the security organization
- Maintains security policy documentation and ensures that necessary changes are incorporated as directed by the architect or management

Security Investigator

This position is responsible for Legal, HR, and internal investigations into security incidents, breaches, attacks, and violations. The security investigator often works closely with law enforcement agencies as needed. Skills required include technical expertise as well as evidence handling and forensic procedures. The security investigator may hold industry-related certifications in forensics and incident response.

Among other duties, the security investigator:

- Responds to requests from HR, Legal, and other internal departments to investigate incidents
- Coordinates with outside attorneys or law enforcement representatives
- Collects and preserves evidence from computer systems
- Performs e-discovery and forensic searches for keywords and patterns
- Produces detailed reports on investigations
- Provides information to the HR and Legal departments for action
- Maintains strict secrecy about ongoing investigations

Security Awareness Trainer

The primary role of this position is to develop and deliver security awareness training to the business based on corporate security policy, standards, procedures, and guidelines. The trainer generally has a background in security as well as in education and training. The trainer coordinates and collaborates with the security department subject matter experts to ensure that the training is both comprehensive and accurate. This position may alternatively reside in another department within the business, typically Human Resources or Communications.

An important characteristic of this position is that the skill set required for the delivery of effective security awareness training is not often found within an IT department, yet the position requires detailed security knowledge. Assigning security engineers and security administrators to produce training materials can be ineffective, due to the highly technical nature of their work and the requirement for delivering training in “plain English.” The trainer must be skilled in interpreting technical information for the business’ employees in a way that is understandable, fresh, interesting, and highly relevant.

Facility Security Officer

The primary role of this position is to enforce the business’ physical security policy at each building location. Each major facility location should have a security officer responsible for coordinating all physical security–related activities and incidents at the facility. The person in this position is not the same person who is operationally responsible for the computer equipment at the facility. The facility security officer has the authority to take action without the approval of the management at the facility when required to ensure physical security. This position also typically works within a Facilities department rather than IT.

All physical security reports are reviewed by the facility security officer. For example, this position reviews log files of facility access records, such as key card logs. The facility security officer is responsible for coordinating all activities related to security incidents at the facility and has the authority to decide what actions are to be taken as directed by the incident response procedures. The facility security officer coordinates all activities with the corporate security manager, director, or vice president.

Application Security Functions

In organizations that develop in-house code for applications used internally, depending on the size and complexity of the application development process there may be a justification for at least one application security specialist. This person would need to be highly knowledgeable about the programming languages being used, and well-trained in security programming techniques (as described in Chapters 26 through 30 of this book). The role of this job function is to provide guidance and training to programmers on how to write secure code, and to review every line of code produced by the programmers for security vulnerabilities and flaws. Commercial code scanners and application testing technologies would also be used by the person in this role to scan and test in-house software for flaws. Alternatively, an outside organization may be contracted to perform code reviews and scanning. Code review and sign-off by this security function should be required before promoting any code to production.

Business Continuity and Disaster Recovery Planning Functions

Depending on the size of the business, business continuity planning (BCP) and disaster recovery (DR) planning and testing may be done by one person (in smaller organizations) or several people in each function (in larger organizations). The question of whether these functions belong within the security organization is best determined by the needs of the business. Generally speaking, smaller businesses that have these functions performed by one or two people should place them in the security organization, while larger businesses may benefit from a dedicated organization for BCP and DR. A good rule of thumb is that they should be part of the information security organization if their work is primarily technical in nature, whereas they should reside elsewhere in the business if their focus is more business-oriented than technical. Chapter 32 covers these functions in more detail.

Non-Security Jobs with Security Responsibilities

Several individuals in a business have important responsibilities in the maintenance of security. These individuals may or may not focus exclusively on security in their jobs. Some of these positions are security positions; others are held by people who are responsible for keeping the business secure even if their primary job is something else.

Every IT department has system and network administrators. Sometimes these are the same person; sometimes the duties are divided among different individuals or departments. Regardless of the reporting structure, the system and network administrators bear important security responsibilities. System administrators build new computer systems; install operating systems; install and configure software; and perform troubleshooting, maintenance, and repairs. In the course of all these functions, system administrators apply security standards and policies. Operating systems must be installed in compliance with the security standards for their particular application. This usually includes turning off unneeded services (known as *hardening*), applying the latest security updates and patches, and applying templates and secure configurations to software applications. Any oversight or failure to consider the security of the system can compromise the entire organization, so the system administrator position is crucial to the success of the security program.

Network administrators have responsibilities and levels of access that require them to conform to security standards and policies as well. Often, the network administrator is responsible for firewall and router configurations that apply the business' security policy in specific situations. Incorrect or inappropriate configuration choices can open up security holes that put the entire business at risk.

Data that is resident on computer systems, shared storage devices, databases, and applications must be handled securely. This means encrypting data in storage (or at rest) and data in transit, performing change control, and implementing access controls and authorization levels to ensure that only the right people can get to the information. The operational responsibility for this data security management falls into the domains of the data owners and the data custodians. Data owners make the decisions that determine who should modify, view, change, and create information files. The owner of each piece of data should identify who is the intended audience, who can make changes, and who can erase the data.

The data custodian implements the decisions of the data owner by making approved changes, presenting the data to the appropriate audience, and properly destroying the data when it is deleted. When sensitive data is strongly overwritten, the data custodian ensures that the data is properly destroyed.

Security Incident Response Team

Security incident response teams are known by several names. Some are called SRT for security response team, some are called CIRT for computer incident response team, and some are called IRT for incident response team (which is the term used in the following discussion). Regardless of the specific terminology, these teams are collections of individuals from various parts of the business who are brought together to handle emergencies. They join the team apart from their daily responsibilities in order to prepare, practice, and drill for potential emergencies and, in the event of an actual emergency, handle the situation.

Examples of the types of incidents a response team might handle include

- Hostile intrusions into the network by unauthorized people
- Damaging or hostile software loose on a system or on the network
- Unauthorized access or acceptable use violations resulting in the need for investigations of personnel
- Virus activity
- Software failures, system crashes, and network outages
- Participation in external investigations by law enforcement, government regulators, or international watchdog and legal organizations
- Court-ordered discovery, evidentiary, or investigative legal action
- Illegal activities such as software piracy

Every business performs incident response, whether or not they have an official IRT established. In many businesses where there is no IRT, individual employees perform incident response by dealing with incidents in their own way. A software virus outbreak is one example. In businesses without an IRT, employees may choose to install antivirus software, run specialized virus cleaning software, or just live with a virus infestation. In these situations, no coordination happens and virus response varies with each individual, usually without enterprise-wide success. One advantage of an organized IRT is that it can deal with incidents like this on a higher level, with more comprehensive success.

Members of an IRT should include technical experts who can evaluate incidents like network intrusions, software failures, and virus outbreaks on a technical level; administrators who can keep logs and maintain the paperwork and electronic information associated with an incident investigation; managers who coordinate the work of the IRT members; and, if available, IRT specialists who have served on prior IRTs. None of these individuals necessarily needs to be assigned to the IRT as a full-time position. Typically, businesses that establish an IRT leverage employees from many other parts of the business and ask them to share their responsibilities between their regular job and the IRT.

An IRT can be assigned individuals with specific technical expertise in a variety of areas. Depending on the business and the types of technologies used in the infrastructure, this expertise may include

- Virus management
- Hostile software detection and management
- Vulnerability analysis
- Specific hardware platforms
- Specific operating systems
- Commercial off-the-shelf or open source tools and applications
- Custom-developed or in-house-developed software and/or scripts

The IRT should have a clearly defined depth of standard investigations, because investigations become more expensive and time-consuming as they go deeper. The basic investigative lifecycle includes Preparation, Identification, Detection, Eradication, Recovery, and Lessons Learned. The IRT may also need to prioritize its activities, especially in cases where several incidents happen at once, and this prioritization should be directed by management rather than the individual team members, to keep the team aligned with the corporate goals.

Daily IRT operations can include interpretation of reported incidents; prioritization and correlation with existing efforts; evaluation of current trends and industry experiences; verification that incidents are real; categorization of incidents; and summarization and reporting to management, end users, and outside agencies. Once incidents are identified and evaluated, removal of the cause by blocking or fixing the exploited vulnerability and restoration of the original state of the impacted system or network can be performed. During the entire process, a careful log and audit trail should be preserved, and information gathered should be evaluated to determine how to improve IRT operations in the future (and this information may be required for legal purposes if prosecution is pursued).

Many aspects of an IRT's actions can be identified, categorized, and codified. These actions should be documented as part of an operational procedure manual. This allows individual team contributors to make informed and appropriate decisions during the heat of an incident. Operational procedures can include standard incident response process, vulnerability analysis and remediation, communication with other groups and with the general business entity, coordination with law enforcement and the court system, and evidence handling and audit trail maintenance.

Many businesses want to have their own in-house IRT, so the team can integrate into the corporate culture and become more informed and effective. Others prefer to outsource this function to avoid having to hire incident response specialists. Outsourcing carries the additional advantage of pay-as-you-go, where costs associated with incident response occur only when the IRT is activated during an incident. Incident handling should be done according to a consistent set of well-documented procedures, in case a court proceeding is required. Investigation manuals are available from a variety of sources that can be used to guide the investigator.

Managed Security Services

Most organizations, whether large or small, have difficulty achieving a high enough level of information security to comply with industry best practices. Very few businesses invest in an internal security organization with enough resources to do everything the business would like to do. Most businesses realize this but continue to do business with the hope that nothing bad will happen.

However, more businesses are beginning to recognize the value of outsourcing services that are not central to their core business. It's rare for modern businesses to hire their own cafeteria staff or housekeeping staff or, in many cases, even handle their own payroll. It would be unthinkable for most businesses to maintain a force of air transportation. Now, other types of services are beginning to come under the same scrutiny for efficiency, quality, and cost-effectiveness.

Managed Security Service Providers (MSSPs), outside firms contracted by businesses to perform specific security tasks, are becoming increasingly popular and viable for modern businesses. These firms are businesses that hire specialized staff with expertise in focused areas such as firewall management, intrusion-detection analysis, and vulnerability analysis and remediation. Often, these companies are able to hire specialists that are more advanced than what other businesses can afford, because of their specialization. Their customers are then able to gain access to this expertise without having to pay the salaries and infrastructure costs, which are absorbed by the MSSP.

There are four good reasons to look to an information security provider for outsourced services:

- Security expertise is not found in-house.
- Security is required 24×7×365 while functionality may be required only for certain business windows (for example, 8 A.M. to 5 P.M.).
- Vast amounts of data must be examined.
- Specialized skill sets are hard to find.

A security infrastructure requires constant vigilance. It's not enough to rely on automated software that can be tricked, or might crash, or may overlook important scenarios. Human intelligence is needed to analyze activity and make decisions on the spot. It's not enough to have one person with a mobile phone—three shifts are required. Moreover, intruders don't take vacations, and they attack from all the different time zones.

Identifying security threats and making decisions about how to respond involves sifting through log files, network activity, and configurations. False positives, true positives, false negatives, and true negatives are all possible outcomes from an inspection—one system communicating legitimately with another may appear to be an attack, or a system administrator performing a routine upgrade may look like an intruder. Somebody needs to be able to investigate these situations properly to determine the most appropriate response.

All of this requires advanced skills. Experienced security specialists are hard to find, but security service providers can attract senior-level staff because the people who specialize in security are attracted to businesses that focus on their field of expertise.

MSSPs must adhere to an organization's policy, standards, procedures, and guidelines and should be subject to auditing.

Outsourcing security functions to MSSPs changes the business equation from one of running and managing a 24×7 operation in an in-house shop to vendor management. Most businesses are more experienced with the latter than the former, but the key to success is to manage the vendor properly to meet the expectations and needs of the business. There are pros and cons associated with outsourcing security operations to MSSPs.

Benefits and advantages include

- Experience
- Cost savings
- Fast implementation
- Adaptability
- Infrastructure

Liabilities and disadvantages include

- Delays in processing events and incidents
- Failure to adhere to service level agreements
- Performance that does not meet expectations
- Inability to perform timely investigative responses
- Inability to align to the primary business' mission and business objectives

When information security is the primary business of an organization, that organization will have a strong business motivation to invest in a world-class security infrastructure. In addition, that organization will work with many different customers with widely varying environments, and it will implement many different types of security solutions. Information security providers bring this experience to bear in their customers' environments, providing a level of quality that can't be matched by organizations that don't specialize in security.

In general, service providers may save their customers money by performing a service more efficiently than the customers can perform it on their own. Service providers leverage their staff of specialists to service many different accounts, thus giving everyone the benefit of industry leadership. Additionally, they often produce methodologies, best practices, and standards that can be applied in their business relationships. These business tools often enable service providers to provide significant cost savings to their customers.

Many projects fall behind schedule or have difficulty getting off the ground due to lack of resources, management support, financing, or effective project management. Service providers often avoid these problems by applying all these components in a focused way to the projects on which they are engaged. Service providers have a strong business motivation to succeed in the projects they take on.

Because security providers work with many different technologies and products, they have a level of flexibility often denied to other organizations. The number of security specialists most organizations can afford to employ is usually much smaller than the number a security provider can afford to employ, and the former's staff usually has a skill set that is limited to the products with which the staff members have personally worked. This gives service providers the advantage of flexibility, since their staff is larger and more focused on the task at hand.

Unlike with most organizations, the information security infrastructure of a security provider is revenue-generating rather than an expense. For that reason, the security provider can apply a greater amount of resources to developing its infrastructure and can leverage that infrastructure to the advantage of the customer. Security providers have the motivation to spare no expense to produce a world-class infrastructure, and their customers reap the benefits.

Services Performed by MSSPs

On Internet connections, wide area networks, and local area networks, MSSPs provide

- Incident detection
- Incident logging
- Proactive response
- Reactive response

Different zones of an organization's data network can be monitored and managed from a security perspective. Typically, these can include the corporate LAN, the WAN connections to remote sites, and connections over public networks such as the Internet and even cloud services. Many organizations have virtual private networks (VPNs) to connect employees to their network or to connect other sites, and many organizations also have extranet connections to partners, service providers, and customers.

Each of these zones should be managed and monitored from a security perspective, and each should adhere to strong security principles. Each will have differing requirements for access and privacy. Whenever a problem occurs, such as unauthorized access or misuse, detecting the incident is crucial to the success of an organization's security. Recent data losses by some well-known companies were not detected right away and left those companies embarrassed after the incidents were reported in the press. In some highly publicized cases, those companies did not know for several weeks that they were taken advantage of.

Potentially even more important than the loss of PR is the loss of opportunity when incidents go undetected. Security violations that are detected right away can be dealt with *during the incident*, which not only affords the opportunity to shut down the attack before serious harm occurs, but also prevents the loss of credibility that is crucial to many organizations' customer relationships. Incidents in progress can also be logged in detail for potential legal action or for further investigation after the incident has concluded.

Many organizations desire proactive response, which is to say, prevention of security violations before they take place. Blocking attacks while continuing to perform logging of data can be of great value to an organization. Reactive response is also important; it usually involves human interaction to determine what course of action is best for the business, up to and including disconnection of service—a decision that might cost an organization thousands of dollars in lost revenue but may save millions in lost data. Decisions like that require a quick link between the people monitoring the security and the people making the business decisions.

Services That Can Be Monitored by MSSPs

Security service providers can provide monitoring of many different types of activities. MSSPs will typically monitor the network for unusual or suspicious activity and identify anything that requires direct intervention or incident response. In such cases, they either raise an alert to IT or information security staff, or they may perform a direct intervention if they have the access and ability (and the contract provides this service). The activities that may be monitored by an MSSP include

- Unauthorized access attempts to firewalls, systems, and network devices
- Port scanning
- System intrusion detection originating from a protected system behind a firewall
- Network intrusion detection originating from "probe" devices connected to the protected internal network
- Root and administrator account usage
- Denial of services
- Other relevant security events

Many security service providers can also provide additional value-added services, such as:

- Detection of nonstandard behavior of services
- Detection of changes to systems
- Reduction of false alarms by employing human intelligence
- Correlation between events on the internal network and the Internet
- Providing updates of the latest security products, threats, and vulnerabilities
- Scanning and reporting on vulnerabilities
- Support and training

Many organizations want to know about authorized as well as unauthorized activities. Managing a data infrastructure is a complex business, and knowing what constitutes a normal pattern of behavior can be a significant asset to managers.

Security Council, Steering Committee, or Board of Directors

The security organization should be included in all efforts that involve corporate data and resources. Many different departments handle data, not just IT. For example, the HR department handles confidential employee information. The Legal department handles confidential business and customer information. The Facilities department may handle badging and physical access. Generally speaking, every major department in the business has some level of interaction with business resources and data. All of these departments should coordinate with the security organization. In most businesses, the security team meets with almost every manager of the business, and sometimes with most of the employees.

A security council or steering committee, whose members include representatives from each major business department, provides a forum for information exchange that facilitates the job of the security practitioner and identifies business requirements to which the security organization should be privy. Each security council representative provides status updates of initiatives within that representative's organization, and each receives information from the security organization about initiatives and practices that impact each of them.

The security council can be used in a variety of ways. Information gathering is one important opportunity. Members of the security council have unique visibility into the operation of their part of the business. This visibility is important to the comprehensiveness of the security practitioner's focus. For example, a department that is considering a new technology initiative may not have considered the security impact on the rest of the network, but the security practitioner, upon hearing about the initiative, may make conceptual connections overlooked by the individual department.

A security council or steering committee can also be an effective risk management tool. The purpose of a risk analysis is to identify as many business risks as possible, and then either accept, mitigate, or transfer those risks. Any risks that are overlooked by a risk analysis put the business in jeopardy if any of those risks become realized. Members of the security council can be polled to identify specific business risks in each of their specialties, and this provides a risk analysis with a greater scope and better coverage.

Another advantage is that it gives a sense of participation and teamwork to business departments that may otherwise act independently without consulting each other, or even compete for resources or produce conflicting infrastructures.

Interaction with Human Resources

Human Resources departments need to provide required information about new hires to security administrators before the new hires' start date. This is an important interaction between HR and IT, even if the security organization is not part of the hiring procedure. Security administrators need to know at any point in time whose employment with the business is valid, so they can properly maintain and monitor accounts on systems and on the network. Perhaps even more important, HR also reports required information about terminations to system administrators before the final termination occurs. The security organization is always involved in terminations to some extent, because employee terminations result in the revocation of trust. When trust is revoked, assurance must be provided that all access has been revoked, and activity must be monitored to ensure the maintenance of that revocation.

HR manages contractor information and provides this information to security administrators. Contractors, as temporary employees, present special problems to security administrators. They often work for only a short time and sometimes come and go, resulting in a constant process of granting and revoking physical access and system and network accounts. It's hard to tell when seeing a contractor in the hallways whether they should be there or not. The security of the network relies heavily on the timely transfer of information from HR to the security organization. HR, in turn, requires timely information from individual managers regarding the status of their contractors hired directly and managed individually.

HR performs background checks, credit checks, and reference checks on new employee applicants. Exit interviews are conducted with terminating employees to recover portable computers, telephones, smart cards, business equipment, keys, and identification badges and to identify morale problems if they exist. Employees discharged for cause must be escorted from the premises immediately and prohibited from returning, both to reduce the threat of retaliation and to forestall any questions if unexpected activity occurs on the network or on the premises.

Monitoring the activities of employees is a matter of corporate culture—those organizations that want to do it differ in the extent and type of response they choose. Likewise, the treatment of confidential and private information differs from business to business, but these are issues that should be dealt with by every organization. If an organization hasn't gotten around to a formal policy on these issues, the best time to start is now, before a policy violation occurs when there is no clear, documented policy that has been communicated to all employees. Communication is truly the key to successful security management. Physical security should not be overlooked, and periodic fire drills can be used to test security measures, help close any gaps, and avoid the danger of having a false sense of security.

Summary

Every business needs a risk management approach that is headed by a top level organization, dedicated to risk management and information security. This organization requires executive-level representation in the business, because the management of risks related to information security is ultimately the responsibility of senior management—whether the business is regulated or not, the top executives are on the hook for any consequences that occur due to failure of security controls. The CSRO or CISO is the highest level of security manager in midsize and larger businesses, with ultimate responsibility for all security efforts for the business. Regardless of the specific functions within the security organization, the definition of who does what should be well defined in an org chart with clear responsibilities assigned to each individual, so security can be properly managed. Security functions include strategic positions such as management, architecture, and policy specialists, as well as operational positions such as administrators, analysts, and investigators. Other functions such as BCP, DR, and physical security may also reside within the information security organization, depending on the nature of the business.

In addition to these full-time roles, security response teams are comprised of collections of individuals from various parts of the business who are removed from their daily responsibilities and brought together to prepare, practice, and drill for emergencies, and these are the people who handle emergencies when they arise. Further, a corporate security council or steering committee, whose members include representatives from each major department in the business that are stakeholders in the end result of the security program, provides a forum for information exchange and input into the decisions that shape the security program.

For those functions not staffed internally, MSSPs are an option. These outside firms are contracted by businesses to perform specific security tasks such as monitoring, alerting, and incident response. MSSPs are becoming increasingly popular for many security roles because they can be less expensive, more efficient, and more effective than what many businesses are capable of building in-house (especially for 24 × 7 service).

References

Bassett, Jackie, and Dan Rothman. *A Seat at the Table for CEOs & CSOs*. Digital edition. AuthorHouse, 2007.

Collette, Ron, Michael Gentile, and Skye Gentile. *CISO Soft Skills: Securing Organizations Impaired by Employee Politics, Apathy, and Intolerant Perspectives*. Auerbach Publications, 2008.

Erbschloe, Michael. *The Executive's Guide to Privacy Management*. McGraw-Hill/Osborne, 2001.

Fitzgerald, Todd, and Micki Krause. *CISO Leadership: Essential Principles for Success*. (ISC)2 Press, 2007.

Gentile, Michael, Ron Collette, and Thomas August. *The CISO Handbook: A Practical Guide to Securing Your Company*. Auerbach Publications, 2005.

Kovacich, Gerald L. *The Information Systems Security Officer's Guide*. 2nd ed. Butterworth-Heinemann, 2003.

Lam, J. "Enterprise-Wide Risk Management and the Role of the Chief Risk Officer." *ERisk.com*, March 25, 2000.

Soo Hoo, K. "How Much Is Enough? A Risk-Management Approach to Computer Security." Presented at the Workshop on Economics and Information Security, University of California at Berkeley, May 2002.